--20. A method for protecting the processing of sensitive information in a security module having a monolithic structure, information processing means (31) and storage means for storing (32,33) information capable of being processed by said processing means, comprising the following steps:

- selecting a piece of sensitive information stored in the storage means;
- determining a specific condition for the integrity of said information;
- reading the information and transmitting it to the processing means for processing;
- processing the information and verifying during processing that the specific condition is satisfied; and
- disabling processing of the information if the specific condition is not satisfied.

21. The method according to claim 20, wherein the information is an operation code read in the storage means (32, 33), the operation code being contained in a table having a content determined during the manufacture of the security module, and the specific condition for the integrity of the information being the value of the information is equal to one of several set values.

22. The method according to claim 21, wherein the operation code to be processed is coded in the form of data bits and said bits do not all have the same binary value.

23. The method according to claim 20, wherein the specific step of determining the condition for the integrity of said information comprises checking a calculated or first piece of integrity data using the information read in the storage means (32, 33) during the reading of the information and transmitting the first piece of integrity data to the processing means, and calculating a second piece of integrity data by the processing means from the information received and checking for equality between the first and second pieces of integrity data.

24. The method according to claim 23, wherein the first piece of integrity data is calculated from at least one piece of calculation data whose value varies as a function of time.

25. The method according to claim 23, wherein the first piece of integrity data is calculated from at least one piece of calculation data whose value varies randomly.

26. The method according to claim 20, wherein the disabling of the processing of the information is performed by a microprogrammed instruction.

27. The method according to claim 26, wherein the microprogrammed instruction performs the following steps:

- writing a piece of disable data into a nonvolatile location of the storage means (32, 33); and
- disabling the processing of the information.

28. The method according to claim 27 further comprising reading by the processing means (31) a nonvolatile location of the storage means (32, 33) upon power up of said module and disabling the module if a value read at this location does not match.

29. A security module comprising an electronic circuit having a monolithic structure and comprising information processing means (31) and information storage means (32, 33), means for extracting information from the storage means and means for selecting information to be processed, the processing means further comprising means for verifying a specific integrity condition of a piece of sensitive information, and means for disabling the processing of the information, said means for disabling being activated when the means for verification have detected that the specific condition is not satisfied.

30. A security module according to claim 29, wherein the processing means (31) execute instructions corresponding to operation codes extracted from a table, characterized in that the table comprises a forbidden instruction value.

31. A security module according to claim 30, wherein the operation code to be processed is coded in the form of data bits, the security module comprising a means for reading the values of all the bits and a disabling means activated when the values of the bits are all identical.

32. A security module according to claim 29, wherein the processing means (31) execute instructions corresponding to operation codes extracted from a table, the security module comprising a means for reading an operation code and a disabling means activated during the reading of a forbidden operation code.

33. A security module according to claim 32, wherein the disabling means comprise a means for irreversibly writing an indicator into the storage means (32, 33), and a means for reading said indicator during the next power-up of the module.

34. A security module according to claim 29, comprising parity generators (7, 8) cooperating with the storage means, parity generators (11) cooperating with the processing means, and a comparator connected to each of the parity generators and capable of inducing an interrupt in the processing means.

35. A security module according to claim 34, wherein the operation of the parity generators (7, 8) varies as a function of time.

36. A security module according to claim 34, wherein the operation of

the parity generators (7, 8) varies randomly.

A2 Cncld.

37 A security module according to claim 33, characterized in that the irreversible writing of the indicator into the storage means (32, 33) is performed by executing a microprogrammed instruction.

38. A security module according to claim 29, characterized in that the security module is a microcircuit card.--